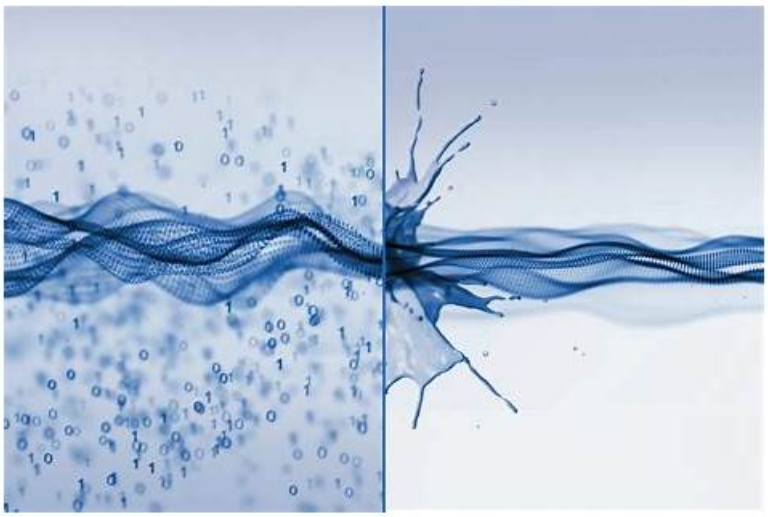
Valid Digital-Forensics-in-Cybersecurity Vce Dumps | Digital-Forensics-in-Cybersecurity Labs



P.S. Free & New Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by Fast2test: https://drive.google.com/open?id=1ua-Bpeb_8G1MbUFgb3WTKfW3M8WUejkO

We have three versions packages of the Digital-Forensics-in-Cybersecurity exam questions to help you comprehensively. Also, all contents are carefully prepared by our researchers. So you needn't to read and memorize the boring reference books of the Digital-Forensics-in-Cybersecurity Exam. Most people have successfully passed the exam under the assistance of our study materials. So try to trust us. Our Digital-Forensics-in-Cybersecurity study materials will help you generate a wonderful life.

If you study with our Digital-Forensics-in-Cybersecurity exam questions, you are bound to get the certification. The scientific design of Digital-Forensics-in-Cybersecurity preparation quiz allows you to pass exams faster, and the high passing rate will also make you more at ease. In this age of anxiety, being able to meet such a product is really fortunate for you. Choosing Digital-Forensics-in-Cybersecurity training engine will make you feel even more powerful. You can improve your ability more easily. When others work hard, you are already ahead!

>> Valid Digital-Forensics-in-Cybersecurity Vce Dumps <<

Digital-Forensics-in-Cybersecurity Labs | Latest Digital-Forensics-in-Cybersecurity Exam Pattern

The competition in today's society is the competition of talents. Can you survive and be invincible in a highly competitive society? Can you gain a foothold in such a complex society? If your answer is "no", that is because your ability is not strong enough. Our Digital-Forensics-in-Cybersecurity test braindumps can help you improve your abilities. Once you choose our learning materials, your dream that you have always been eager to get WGU certification which can prove your abilities will realized. You will have more competitive advantages than others to find a job that is decent. We are convinced that our Digital-Forensics-in-Cybersecurity Exam Questions can help you gain the desired social status and thus embrace success.

WGU Digital-Forensics-in-Cybersecurity Exam Syllabus Topics:

Topic	Details
Topic 1	• Domain Evidence Analysis with Forensic Tools: This domain measures skills of Cybersecurity technicians and focuses on analyzing collected evidence using standard forensic tools. It includes reviewing disks, file systems, logs, and system data while following approved investigation processes that ensure accuracy and integrity.

Topic 2	• Domain Digital Forensics in Cybersecurity: This domain measures the skills of Cybersecurity technicians and focuses on the core purpose of digital forensics in a security environment. It covers the techniques used to investigate cyber incidents, examine digital evidence, and understand how findings support legal and organizational actions.
Topic 3	• Domain Incident Reporting and Communication: This domain measures the skills of Cybersecurity Analysts and focuses on writing incident reports that present findings from a forensic investigation. It includes documenting evidence, summarizing conclusions, and communicating outcomes to organizational stakeholders in a clear and structured way.
Topic 4	• Domain Recovery of Deleted Files and Artifacts: This domain measures the skills of Digital Forensics Technicians and focuses on collecting evidence from deleted files, hidden data, and system artifacts. It includes identifying relevant remnants, restoring accessible information, and understanding where digital traces are stored within different systems.
Topic 5	• Domain Legal and Procedural Requirements in Digital Forensics: This domain measures the skills of Digital Forensics Technicians and focuses on laws, rules, and standards that guide forensic work. It includes identifying regulatory requirements, organizational procedures, and accepted best practices that ensure an investigation is defensible and properly executed.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q39-Q44):

NEW QUESTION # 39
Which Windows 7 operating system log stores events collected from remote computers?

- A. Application
- B. System
- C. ForwardedEvents
- D. Security

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
TheForwardedEventslog in Windows 7 is specifically designed to store events collected from remote computers via event forwarding. This log is part of the Windows Event Forwarding feature used in enterprise environments to centralize event monitoring.
* TheSystemandApplicationlogs store local system and application events.
* TheSecuritylog stores local security-related events.
* ForwardedEventscollects and stores events forwarded from other machines.
Microsoft documentation and NIST SP 800-86 mention the use of ForwardedEvents for centralized event log collection in investigations.

NEW QUESTION # 40
A victim of Internet fraud fell for an online offer after using a search engine to find a deal on an expensive software purchase. Once the victim learned about the fraud, he contacted a forensic investigator for help.
Which digital evidence should the investigator collect?

- A. Whois records
- B. Email headers
- C. Computer logs
- D. Virus signatures

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

In Internet fraud investigations, computer logs are critical because they provide a record of user activity, including browsing history, downloads, and system events. These logs can help establish a timeline, identify malicious access, and confirm fraudulent transactions.
* Computer logs may include browser history, system event logs, and application logs that document the victim's interaction with the fraudulent offer.
* Whois records help identify domain registration details but are secondary evidence.
* Email headers are relevant if communication via email was part of the fraud but less critical than logs that show direct interaction.
* Virus signatures are used in malware investigations, not directly relevant to fraud evidence collection.
Reference:According to guidelines by the International Journal of Digital Crime and Forensics and the SANS Institute, capturing logs is essential in building a case for Internet fraud as it provides objective data about the victim's system and activities.

NEW QUESTION # 41
A forensic scientist is examining a computer for possible evidence of a cybercrime.
Why should the forensic scientist copy files at the bit level instead of the OS level when copying files from the computer to a forensic computer?

- A. Copying files at the OS level will copy extra information that is unnecessary.
- B. Copying files at the OS level changes the timestamp of the files.
- C. Copying files at the OS level takes too long to be practical.
- D. Copying files at the OS level fails to copy deleted files or slack space.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Bit-level (or bit-stream) copying captures every bit on the storage media, including files, deleted files, slack space (unused space within a cluster), and unallocated space. This ensures all digital evidence, including artifacts not visible at the OS level, is preserved for analysis.
* Copying at the OS level captures only allocated files visible in the file system, missing deleted files and slack space.
* Bit-level copying is a cornerstone of forensic best practices as specified in NIST SP 800-86 and SWGDE guidelines.
* Timestamp changes and unnecessary information issues are secondary concerns compared to the completeness of evidence.

NEW QUESTION # 42
The following line of code is an example of how to make a forensic copy of a suspect drive:
dd if=/dev/mem of=/evidence/image.memory1
Which operating system should be used to run this command?

- A. Windows
- B. Unix
- C. MacOS
- D. Linux

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The 'dd' command is a Unix/Linux utility used to perform low-level copying of data, including forensic imaging. It allows bit-for-bit copying of drives or memory, making it a common tool in Linux-based forensic environments.
* Windows does not natively support 'dd'; similar imaging tools are used there.
* The command syntax and file paths indicate Linux/Unix usage.
Reference:Digital forensics training and NIST SP 800-101 mention 'dd' as a reliable imaging tool in Linux forensic workflows.

NEW QUESTION # 43
Where does Windows store passwords for local user accounts?

- A. SAM file in Windows\System32
- B. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

- C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces
- D. Security file in Windows\System32

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Windows stores the hashes of local user account passwords in the SAM (Security Account Manager) file, which is located in theWindows\System32\configdirectory. This file is a critical component in the Windows security infrastructure.
* The registry paths in A and B refer to network profiles and wireless configuration data, unrelated to password storage.
* The "Security" file also resides in theSystem32\configfolder but stores security policy data rather than password hashes.
* The SAM file stores password hashes and is targeted in forensic investigations for credential recovery.
Reference:Microsoft technical documentation and NIST digital forensics standards explain that the SAM file is the definitive source for local user password hashes in Windows systems.

NEW QUESTION # 44
.....

Our WGU Digital-Forensics-in-Cybersecurity practice materials from our company are invulnerable. And we are consigned as the most responsible company in this area. So many competitors concede our superior position in the market. Besides, we offer some promotional benefits for you. The more times you choose our WGU Digital-Forensics-in-Cybersecurity Training Materials, the more benefits you can get, such as free demos of our Digital-Forensics-in-Cybersecurity exam dumps, three-version options, rights of updates and so on. So customer orientation is the beliefs we honor.

- www.stes.tyc.edu.tw, victoracyi631108.prublogger.com, socialicus.com, isaiahxzyd494038.smblogsites.com, worldlistpro.com, www.stes.tyc.edu.tw, haimacnvj397399.blog2news.com, karimjbxe897896.blognody.com, socialaffluent.com, poppieijbs681709.ziblogs.com, Disposable vapes

What's more, part of that Fast2test Digital-Forensics-in-Cybersecurity dumps now are free: https://drive.google.com/open?id=1ua-Bpeb_8G1MbUFgb3WTKfW3M8WUejkO